

ATTACHMENT 4

The Background Investigation (BI) process shall be followed for all contractors and subcontractors within the accreditation boundary. The BI process for all of the contractors and subcontractors outside of the accreditation must either comply with the BI process as described within this document or a contractor defined and ETS2 PMO approved commercially equivalent BI process. Regardless of which BI process is selected, all contractors and subcontractors/teaming partners must adhere to a BI process.

Personnel Background Investigation Requirements

The contractor will require access to Government sensitive information and/or access to Government information systems. All contractor personnel with access to data or systems within the accreditation boundary must successfully complete, at a minimum, a National Agency Check with Written Inquiries (NACI or equivalent Tier 1) in accordance with Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1K and GSA Directive 9732.1D Suitability and Personnel Security for background investigations to provide services under this contract. The required background investigations for administrative (low risk) personnel shall be a minimum of a Tier 1 (T1) – formerly - National Agency Check with Written Inquiries (NACI) – and for technical staff and personnel who handle Personal Identifiable Information (PII) or government sensitive information shall be a Tier 2 (T2S) – formerly Moderate Risk Background Investigation (MBI) – background investigation. The COR shall identify all individuals who require system accounts and verify that they have successfully completed the required background investigations prior to providing them access to Government sensitive information or information systems.

Incorporated by reference is the Contractor Background Processing Procedures, Version 2, dated August 2, 2017, containing specific instructions on the background investigation processing procedures. Updates to these procedures will be posted to the Concur site where Requesting Official Contractor Employee Approval List (ROCAL) and Contractor Information Worksheets (CIWs) are processed and tracked. Concur is responsible for ensuring that it is adhering to current procedures and using current forms.

Protection of Government Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of this contract. The contractor shall implement procedures that ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of sensitive government information data, and/or equipment. The contractor's procedures shall be consistent with Government and GSA policies, including GSA order 2100.1K, Information Technology Security Policy, OMB Circular A-130, Management of Federal Information Resources, OMB M-06-16, HSPD-12, and the Privacy Act to the extent required by and consistent with Section C. In addition,

during all activities and operations on Government premises the contractor shall comply with the procedures, policies, rules and regulations governing the conduct of personnel or protection of Government facilities and data as expressed by GSA, written or oral.

As applicable, contractor personnel requiring access to the Requesting official Contractor Approval List (ROCAL) and GSA FAS networks shall possess a gsa.gov email address and GSA HSPD-12 Managed Service Office (MSO), Personal Identity Verification (PIV) credential and shall take the **Annual GSA IT Security Awareness Training.**

(END)

THIS PAGE INTENTIONALLY LEFT BLANK